BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan ilmu pengetahuan pada bidang teknologi jaringan terjadi sangat cepat karena mengikuti perkembangan kebutuhan manusia. Salah satu teknologi jaringan yang saat ini menarik perhatian masyarakat adalah teknologi *wireless*. Beberapa perangkat elektronik terkini yang sering digunakan masyarakat juga menggunakan teknologi *wireless*. Salah satu contoh perangkat yang menggunakan teknologi *wireless* adalah WSN(*wireless* sensor *network).* WSN merupakan jaringan dari kumpulan sensor yang terhubung menggunakan teknologi *wireless* secara *ad-hoc* dan setiap sensor *node* digunakan untuk proses pengumpulan data dan menghubungkan dengan *node* yang lain melalui jaringan *wireless.*[1]

Dalam sistem WSN terdapat jaringan dengan *node* bergerak dan *node* tidak bergerak yang memiliki fungsi yang beragam. Untuk WSN dengan *node tidak* bergerak contohnya adalah monitoring suatu lingkungan, sedangkan untuk WSN dengan *node* bergerak contohnya adalah monitoring keadaan hewan dengan menempelkan *sensor node* pada hewan. Karena pada kebanyakan kasus aplikasi WSN digunakan pada lingkungan yang ekstrim dan sensor *node* harus dapat beroperasi secara otomatis tanpa campur tangan manusia, jaringan ini menjadi rentan akan beberapa ancaman jaringan dan dapat mempengaruhi performa dari jaringannya. [2]

Untuk menangani ancaman jaringan pada WSN, dibutuhkan sistem keamanan yang memudahkan transfer data antar *node* dalam jaringan sebagai contoh terdapat beberapa teknik kriptografi dan teknik keamanan lain untuk mengamankan jaringan WSN. Meskipun sudah ada pengenkripsian data menggunakan kriptografi, jaringan masih belum sepenuhnya aman karena penyerang juga dapat menyerang data yang sudah di enkripsi yang menyebabkan keamanan pada data intregasi menjadi lemah. [1]

Terdapat banyak jenis serangan dalam WSN, salah satunya yang paling umum adalah *Sybil Attack.* Dalam serangan ini penyerang menggunakan *node* yang

tidak termasuk dalam jaringan atau bisa disebut *malicious node, node* ini menyerang dengan cara mendapat informasi algoritma *routing* dari *node* asli pada jaringan dan menyamar menjadi *node* yang terdapat dalam jaringan[3]. Lalu ada satu lagi jenis serangan yang menyerupai *Sybil attack*, serangan tersebut adalah *Hello flood Attack.* Dalam serangan ini penyerang menggunakan *malicious node* untuk menyerang dengan cara mengirim *hello request* ke *node* yang asli dalam jaringan secara terus menerus yang akan menyebabkan gangguan pada sistem keamanan[4]. Meskipun terdapat banyak algoritma pendeteksi dan pencegah *malicious node*, tetapi kebanyakan algoritma tersebut mempunyai banyak kekurangan yang menyebabkan kegagalan mendeteksi penyerang dalam jaringan.

Dari penelitian sebelumnya oleh Sher Anusha dengan judul *Simulation of attack in a Wireless* Sensor *Network using NS2* yang meneliti tentang simulasi dari beberapa serangan dalam WSN, penulis mencoba memberi kontribusi dengan menambahkan beberapa parameter penelitian. Dalam penelitian ini, akan diteliti performa WSN saat diserang oleh *Sybil attack* dan *hello flood attack* dengan cara mengukur *throughput*, PDR(*packet delivery ratio*), *jitter* dan *delay* dalam jaringan WSN. Penelitian ini juga menganalisa jumlah *node* dan penyerang dalam jaringan WSN dalam jumlah yang bervariasi dan memandingkan hasil dari masing-masing jumlah *node,* lalu akan di analisa perbandingan dampak yang ditimbulkan pada WSN. *Routing protokol* yang digunakan dalam penelitian jaringan WSN ini adalah *protokol* AODV(*ad-hoc on demanc vactor)*. *Routing* AODV pada jaringan WSN adalah routing jenis *reactive* dimana rute jaringan akan dibuat hanya ketika *node* sumber akan mengirim data ke *node* penerima, disamping itu AODV menggunakan *destination sequence numbers (DSN)* untuk menentukan informasi *routing* yang dikirim *up-to-date* atau tidak dan mencegah perulangan *routing*. Hal ini yang membuat *routing* AODV lebih unggul dari *routing protokol* lainnya[5].

Penelitian ini menggunakan *tools network simulator* (ns-2) simulator untuk menyimulasikan *node* WSN. *Network simulator* merupakan *software* bebasis *open source* yang biasanya digunakan untuk tujuan edukasi dan penelitian. Aplikasi menggunakan dua bahasa pemrograman yaitu C++ dan OTcl(*Object oriented Tool Command Languange*). Bahasa C++ digunakan untuk mekanisme dalam sistem, dan Otcl untuk tampilan *front-end*.[1]Aplikasi ini mensimulasikan jaringan

menggunakan *time-based event*, jadi user dapat menentukan waktu dan kejadian secara *real time*. Dengan aplikasi ini user juga dapat membuat *node* dan pengiriman data antar *node* serta serangan yang terjadi juga dapat dilihat. NS2 dapat digunakan dalam platform unix, mac, dan windows.

Melalui penelitian ini penulis mencoba menganalisa dampak serangan *sybil attack* dan *hello flood attack* dalam jaringan WSN dan membandingkan performa jaringan saat terjadi serangan dan tidak terjadi serangan. Dengan melakukan analisa tersebut, penulis dapat mengetahui karakteristik dari serangan dan performa dari jaringan.

1.2. Rumusan Masalah

Dari latar belakang yang telah diuraikan, didapat permasalahan yang akan diteliti sebagai berikut :

1. Bagaimana performa jaringan WSN apabila terjadi serangan *sybil attack* dan *hello flood attack* pada jaringan WSN.
2. Bagaimana perbandingan dampak serangan *sybil attack* dan *hello flood attack* pada jaringan WSN.

1.3. Tujuan Penelitian

Dari rumusan masalah yang telah diuraikan, maka tujuan dilakukanya Tugas Besar ini yaitu untuk:

1. Melakukan analisa performa jaringan WSN dalam serangan *Sybil attack* dan *Hello flood attack*
2. Membandingkan dampak serangan *Sybil attack* dan *Hello flood attack* pada jaringan WSN
3. Membandingkan kinerja jaringan WSN saat terjadi serangan dan tidak.

1.4. Batasan Masalah

Ruang lingkup permasalahan dalam laporan penelitian ini hanya terbatas pada masalah-masalah sebagai berikut:

1. Jaringan *wireless* yang digunakan adalah jaringan *ad-hoc*.
2. Simulasi jaringan dibuat dengan menggunakan *software* NS2.
3. Membahas performa jaringan dengan tolak ukur *throughput*, PDR, *jitter*, dan *delay*.

4. Membandingkan performa jaringan saat terjadi serangan dan tidak terjadi serangan.
5. Tidak membahas pencegahan dan perlindungan dari serangan *sybil attack* dan *hello flood attack.*

1.5. Metodologi

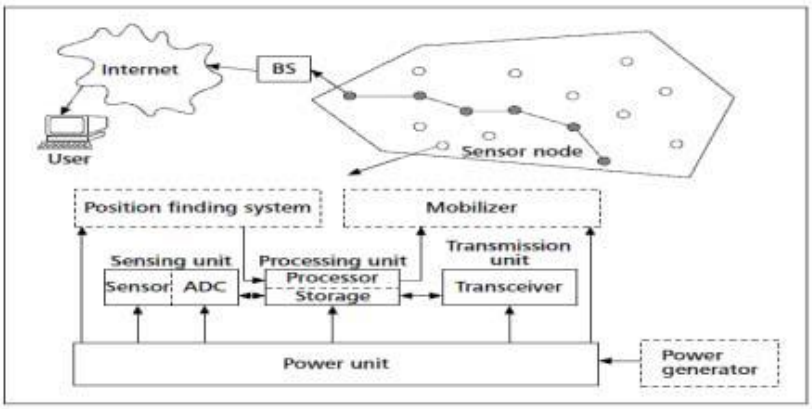
Tahapan yang akan ditempuh untuk mengerjakan Tugas Besar ini diantaranya sebagai berikut:

1.5.1. Studi Literatur

Pada langkah ini dilakukan studi literatur untuk menambah wawasan dengan ilmu yang berkaitan dengan tugas akhir ini yakni *wireless* sensor *network, sybil attack, hello flood attack,* dan *network simulator* 2 . Sumber literatur yang akan digunakan dalam tugas besar ini adalah skripsi, jurnal, dan *internet*.

1.5.2. Perancangan Sistem

Pada langkah ini dilakukan perancangan untuk membentuk jaringan wsn dalam simulator ns-2. Pada dasar desain jaringan wsn terdiri dari power generator untuk menyuplai energi ke power unit, power unit untuk sumber energi saat proses sensing, processing unit, dan transmission unit.[1] Setiap sensor *node* terhubung ke base station yang dapat mengirim dan menerima data. **Gambar 1.1** menunjukkan diagram dasar rancangan jaringan wsn dan arsitektur *node* wsn.



Gambar 1.1 Arsitektur WSN[1]

1.5.3. Implementasi sistem

Pada langkah ini dilakukan implementasi pada jaringan wsn dalam simulator ns-2. Pertama dilakukan konfigurasi simulator untuk menyesuaikan dengan kebutuhan penelitian, lalu membuat *node* pada jaringan dan mengkonfigurasikan *node*. Setelah itu dilakukan simulasi penyerangan oleh *sybil attack* dah *hello flood attack*.

1.5.4. Pengujian sistem

Pada langkah ini, dilakukan pengujian dampak serangan dari kedua jenis serangan yaitu *sybil attack* dan *hello flood attack*. Pengujian ini dilakukan dengan mengukur parameter QoS yaitu *throughput*, PDR, *jitter*, dan *delay* pada jaringan WSN saat terjadi serangan, lalu menganalisa perbandingan dampak pada tolak ukur yang dihasilkan oleh kedua jenis serangan. Hasil analisa dapat digambarkan dalam bentuk tabel *graph*.

1.5.5. Pembuatan Laporan

Pada langkah ini merupakan tahap akhir setelah tahap-tahap sebelumnya sudah selesai. Adapun laporan yang ditulis merupakan seluruh hasil analisis dan pengujian yang telah dilakukan.